Autore: Gianrico Fichera
Release: 1 Gennaio 2021
Release: 1.2 Agosto 2022
Revisione: 1.3 Aprile 2024

La necessità della ridondanza nel datacenter per garantirne l'alta affidabilità

Introduzione

Molto spesso il committente di un progetto per una rete LAN ad alta affidabilità non si rende conto delle motivazioni che rendono necessaria l'implementazione di sistemi complessi e ridondati. E' facile credenza che un sistema hardware di un buon produttore e con ottime specifiche tecniche sia tutto ciò che serva e che quindi lavorerà per anni senza fermarsi mai: ovvero la ridondanza degli apparati e il preoccuparsi della loro manutenzione sia solo uno spreco di tempo e denaro.

Il presente documento tratta in modo teorico il comportamento dei sistemi cercando di calcolare in modo preciso la probabilità che un sistema cessi di funzionare prendendo come esempio le apparecchiature della rete dati del moderno datacenter. A conclusione il documento spiega perchè è necessario utilizzare sistemi di apparati ridondati per garantire gli alti valori di uptime richiesti dai servizi Internet di oggi e perchè un sistema privo di ridondanza non può soddisfare requisiti di alta affidabilità e non può quindi garantire continuità di servizio.

Disponibilità di un sistema

Un pó tutti conosciamo il significato del termine **uptime** in un sistema informatico, ovvero il tempo continuativo da cui un sistema funziona senza interruzioni. Tanto per fare un esempio, nel caso di un Sistema Operativo quale Linux, basta digitare il comando “uptime” per ottenere questo valore oppure il comando “show version” nel caso di un router Cisco. Anche un MacBook ha il comando uptime. In figura degli esempi: MacOSX, Cisco 6500 e Cisco Nexus.

```
gianricofichera — -bash — 80×24
Last login: Tue Jul 24 16:55:52 on console
Gianrico:~ gianricofichera$ uptime
17:22  up 1 day, 27 mins, 2 users, load averages: 1,37 1,41 1,51
Gianrico:~ gianricofichera$
```

```
6506A#show ver | include uptime
_6506A uptime is 21 weeks, 5 days, 7 minutes
```

```
Hardware
  cisco Nexus7000 C7009 (9 Slot) Chassis ("Supervisor Module-2")
  Intel(R) Xeon(R) CPU         with 12224948 kB of memory.
  Processor Board ID JAF1643ABJA

  Device name: genesys1
  bootflash:    2007040 kB
  slot0:              0 kB (expansion flash)

Kernel uptime is 1353 day(s), 23 hour(s), 10 minute(s), 31 second(s)
```

Poichè è impossibile che un sistema non si guasti o che non necessiti di manutenzione, abbiamo bisogno di una misura che ne indichi l'affidabilità includendo la possibilità di interruzioni di servizio.

Introduciamo il concetto di **availability** che è un valore percentuale che misura il tempo in cui un sistema è stato operativo all'interno di un periodo, normalmente un anno. Questo dato quindi considera le criticità in un sistema che lo hanno reso indisponibile e il tempo necessario per la riparazione dello stesso. Vedremo che il valore di availability è un dato fondamentale in fase di progettazione di una rete perchè è il valore che dev'essere massimizzato. In base alle esigenze del cliente è possibile progettare sistemi con valori di availability che possono raggiungere anche il 99.9999%. Dato un valore target di availability si decidono la scelta degli apparati, la tipologia di

manutenzione e assistenza, la topologia di rete e l'ambiente in cui gli apparati devono funzionare.

Partendo dai valori di **uptime/availability** si potrà quindi misurare e certificare l'affidabilità di una rete e di conseguenza si rende possibile la redazione di un **Service Level Agreement** (SLA) ovvero un documento che indichi i livelli di servizio che si possono garantire per una rete specifica.

In generale se una rete non ha un uso continuativo non si includono nella availability i tempi in cui i sistemi sono offline per manutenzione ordinaria o comunque per attività schedulate al di fuori degli orari in cui si utilizzano e quindi in orari che non creano disservizio per l'utenza. E' chiaro che il valore di uptime è irrilevante in un sistema che va volutamente offline senza creare disservizi per l'utenza. Ad esempio se un'azienda di notte non ha nessuna attività lavorativa possiamo prevedere manutenzioni senza compromettere il valore di availability per la rete. E' ovvio però che un guasto non è altrettanto prevedibile.

Dal punto di vista matematico l'availability non comprende le tante variabili che intervengono esternamente al sistema stesso ma che ne determinano un **downtime** ovvero un disservizio. Quindi per quanto perfetta possa essere la progettazione e configurazione degli apparati fisici di rete ci sono cause esterne ad essi che possono comprometterne l'integrità. Queste sono tante e non si possono ignorare. Quindi la premessa al calcolo della availability di una rete è che siano rispettati dei prerequisiti del sistema ospitante la rete stessa, quale il condizionamento o la continuità energetica del CED ospitante.

Ecco un elenco di punti da valutare e prerequisiti dei locali e degli spazi ospitanti i sistemi della rete che se non rispettati impediranno il valore di availabity previsto nella progettazione.

- L'errore umano è percentuale significativa dei problemi che si possono avere in una rete. Il personale che opera e/o farà manutenzione è sufficientemente preparato e con l'esperienza giusta?

- Quanti interventi di riconfigurazione degli apparati sono previsti in un anno? Si tratta di una rete in cui si deve intervenire spesso nei dispositivi? Ci sono dei tempi morti in cui si può intervenire su tali apparati?

- Sono disponibili due linee di alimentazione separate e indipendenti che possono fornire con continuità energia l’una in assenza dell’altra? Sono disponibili gruppi di continuità?

- Gli impianti di climatizzazione e la temperatura sono garantiti nei limiti di servizio degli apparati? Possono esserci guasti? Sono ridondati?

- Le norme relative alla sicurezza (GDPR) per l’accesso ai dispositivi della rete sono applicate in modo corretto in modo da evitare, anche per errore, un danno dovuto ad altre attività di manutenzione su altri apparati adiacenti?

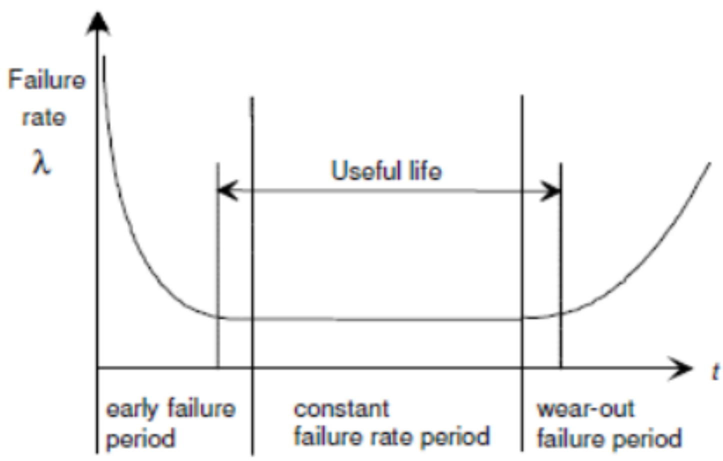
Notate che in alcuni di questi elementi c’è una componente aleatoria e sono di fatto non deterministici. Oltretutto alcuni sono elementi esterni alla rete fisica. Un guasto ad un impianto di climatizzazione non è cosa rara cosí come un problema di alimentazione elettrica.

Il calcolo matematico va affiancato quindi ad un’analisi dell’ambiente in cui si opera e solo a quel punto si potranno fare delle previsioni attendibili.

Il valore di availability è punto di partenza per poter redarre degli SLA con il quale un fornitore di servizi garantisce delle metriche di servizio agli utilizzatori, che si impegna a rispettare. In alcuni casi sono previste delle penali in caso contrario. E’ quindi bene che il fornitore di servizi si faccia bene i conti.

MTBF

L’MTBF è un valore fornito dal produttore di un dispositivo e indica il tempo medio tra due guasti calcolato considerando un insieme di apparati inizialmente funzionanti. Per guasto si intende una condizione in cui un apparato va fuori servizio e necessita di una riparazione. Il fatto che sia un “valore medio” è estremamente importante e da non dimenticare. Un produttore ne calcola il valore con un metodo statistico e quindi il valore fornito è un valore di probabilità e non una certezza. MTBF è un dato valido durante il periodo di vita del prodotto in cui il numero di guasti è pressocchè costante.



Nella nostra trattazione sono due i parametri di interesse:

- **MTBF**: Mean Time Between Failure (tra due guasti)
- **MTTR**: Mean Time to Repaire (da un guasto)
- **MTTF:** Mean Time to Failure (primo guasto)

MTBF è il tempo medio tra due guasti nel caso in cui un apparato fisico sia in condizioni ottimali di funzionamento senza influenze esterne. E' un valore che si utilizza per apparati riparabili.

T= tempo totale di attività
F= numero di guasti

$$MTBF = \frac{T}{F}$$

Se ad esempio si testano 10 apparati per 1000 ore ciascuno e abbiamo tre guasti:

$$MTBF = \frac{1000 * 10}{3} = 3333h$$

Notate che il numero di ore di MTBF non è un numero utilizzabile direttamente. Infatti non possiamo dire che un apparato arriva a lavorare 3333h, potremmo essere oltre il ciclo di vita dello stesso...

I valori di MTBF per un dispositivo possono essere noti solo al suo produttore. Consideriamo quale esempio uno switch L3 Cisco fixed-configuration, quindi con valore ben preciso di MTBF. Nei datasheet possiamo trovare valori di MTBF anche di 390330 ore, come ad esempio nel caso del modello Nexus 93180YC-EX. Questo valore numerico equivale all'incredibile valore di 390000/24h = 16250/365 = 44 anni. Ma che significa? **Non** significa che il prodotto non avrà un guasto per 44 anni. Ecco altri esempi di MTBF in tabella.

Esempi di MTBF in ore di una serie di Swicth fixed configuration		
Cisco 2960S-48FPD-L	183498	740W PoE
Cisco 2960S-48TS-S	357740	No PoE
Cisco 2960S-48LPS-L	205052	370W PoE

Tabella: la complessità hardware riduce il valore di MTBF

Availability

L'**availability** è una misura partendo dal MTBF e dal tempo necessario per la sua riparazione fornisce un valore di disponibilità di un sistema:

$$A = \frac{MTBF}{MTBF + MTTR} \times 100\,\%$$

Ovvero tempo medio per un guasto e tempo di riparazione sono due variabili legate tra loro nella valutazione della continuità di un servizio che un sistema fornirà.

Con un rapido calcolo possiamo vedere che una availability del 98% equivale a 7,3 giorni di downtime per anno. Al 99% siamo a 3,65 giorni. A 99,99 siamo a 52,56 minuti e a 99,999 siamo a 5,2 minuti.

Per migliorare l'availability di un datacenter si devono valutare attentamente i valori MTBF e MTTR delle singole unità che lo compongono. I valori di MTBF sono forniti dai produttori e sono validi solo del loro periodo di vita utlile (**useful life period**), al di fuori del quale il valore di MTBF fornito non è più valido: un prodotto è considerato "vecchio" al di fuori del suo periodo di vita utile e non è più prevedibile un suo guasto.

Il valore di availability è un valore medio che in quanto tale non dipende dal tempo trascorso dalla messa in esercizio di un sistema ovvero e' uguale di anno in anno. Se vogliamo prendere in considerazione il fatto che un sistema invecchia utilizziamo il valore di **reliability** di cui nei paragrafi successivi.

Il tempo e l'usura di un dispositivo

E' incontestabile che maggiore è il tempo di uso di un qualsiasi apparato elettronico e maggiore è la probabilità di un guasto: c'e' un normale invecchiamento di tutte le parti che lo costituiscono e i componenti non sono mai perfetti e quindi il caso ne può determinare una vita inferiore a quella prevista. Ciò dipende anche dalla qualità dei materiali e della componentistica. Se ci limitiamo al periodo di vita utile dell'apparato possiamo immaginare costanti queste variabili: il valore di MTBF è calcolato durante questo periodo.

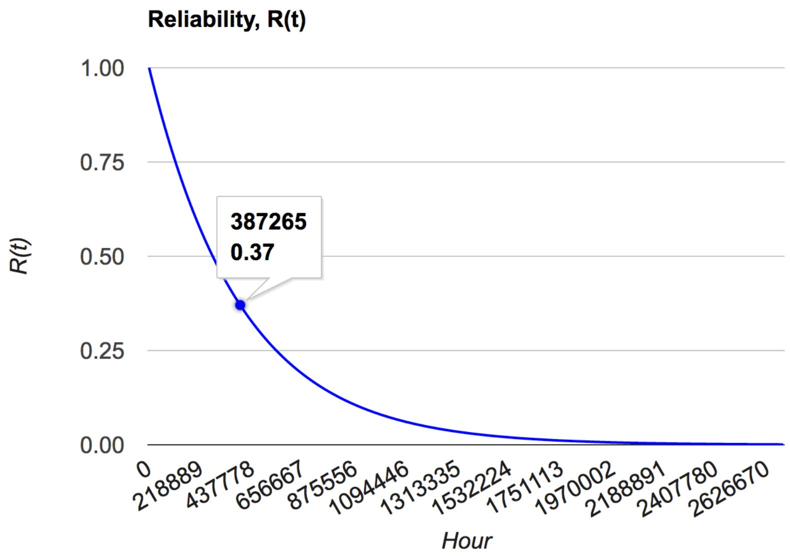
Tanto maggiore è il tempo in cui un sistema è in esercizio maggiore è la probabilità di un guasto. Per più tempo si attende e maggiore è la probabilità che succeda qualcosa insomma. Cerchiamo di formulare matematicamente questo comportamento.

In matematica una funzione il cui tasso di crescita è proporzionale al valore attuale della funzione stessa, si chiama esponenziale. Più il valore in un punto è alto, più la funzione crescerà o decrescerà rapidamente, il che genererà a sua volta una crescita o decrescita maggiore. Pertanto il grafico della funzione esponenziale è curvo verso l'alto e non una linea retta come nel caso delle funzioni proporzionali. **I guasti degli apparati seguono una relazione tra tempo e possibilità di guasto non lineare ma esponenziale.**

Dato un valore di MTBF calcolato su N dispositivi fornito da un produttore è molto utile il valore della probabilità che un singolo dispositivo sia funzionante dopo un certo tempo dalla sua data di messa in servizio.

L’MTBF è un valore medio. Qual’è allora la probabilità che un sistema funzioni al tempo t=MTBF?

Reliability



Consideriamo la funzione esponenziale per calcolare la probabilità di un "guasto" in un sistema. Si introduce la funzione **reliability** R(t):

$$R(t) = e^{-t/MTBF}$$

Il contrario della reliability ovvero la **unreliability** sarà:

F(t)=1-R(t)

Calcoliamo la probabilità che un sistema funzioni al tempo t=MTBF si ha:

$$R(t) = e^{-1} = 0.3677$$

Quindi la probabilità che non ci siano guasti in un intervallo di tempo pari al valore di MTBF è 36.7%. Il che vuol dire che c'e' una probabilità del 63.3% che il sistema sia guasto al tempo t=MTBF!

Il lifetime degli apparati elettronici dovrebbe essere almeno 1/10 dell'MTBF. Il motivo è che si ha un valore di reliability pari al 90% ovvero il 10% di probabilità di guasto:

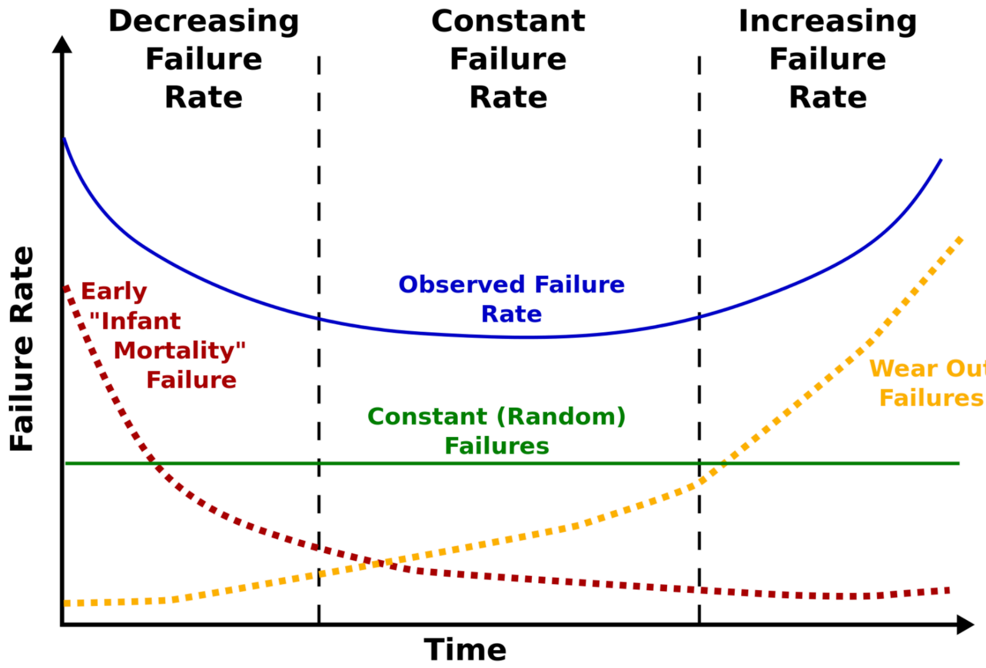
$$R(t) = e^{-1/10} = 0.9$$

Con valori pari a 1/1000 di MTBF volte arriviamo al 99,9%.Questi risultati sono molto importanti e sono molto differenti rispetto a ció che si possa pensare leggendo il solo

$$R(t) = e^{-1/1000} = 0.999$$

Il motivo per cui abbiamo utilizzato la funzione esponenziale nasce dal fatto che i guasti nelle reti dati si possono modellare matematicamente con la **distribuzione esponenziale**. Questa distribuzione descrive fenomeni che non correlati tra loro ovvero è priva di memoria cioè la probabilità di un guasto non è legata al fatto che ce ne siano stati o meno di precedenti, e questa è una valida semplificazione. La formula di cui sopra è derivata dalla distribuzione esponenziale.

L'assunzione che i guasti non sono legati tra loro è considerata ben approssimata se si utilizza un dispositivo nel suo “**useful life period**”, ovvero il suo periodo di vita utile, nel quale il tasso di guasti può essere considerato costante ovvero "**constant failure rate**". Si esce da questa zone appena si inizia ad usare il dispositivo e dopo un lungo periodo di utilizzo.



*This image is a work of a U.S. Army soldier or employee, taken or made as part of that person's official duties. As a work of the U.S. federal government, the image is in the **public domain**.*

Weibull

Ma è possibile matematicamente rappresentare il concetto di invecchiamento di un apparato? Nel mondo reale non si danno garanzie ad un cliente al di fuori del lifetime indicato da un produttore.

Il failure-rate può essere modellato con una funzione "a vasca da bagno" che si chiama **bathtube curve**. Questa puó presentare valori alti all'inizio e dopo il lifetime. E' invece lineare lungo il lifetime. Cosí come molti sistemi si comportano in natura utilizzando la distribuzione esponenziale altri, come quelli che hanno un periodo di vita limitato, si possono modellare con la distribuzione di Weibull. Si noti che le probabilità di guasto di un sistema nuovo, diciamo appena acceso, sono considerate più alte del normale in quando potrebbe esserci qualche difetto grave all'origine.

Per studiare la bathtube curve si puó utilizzare la distribuzione di Weibull. Questa consente di analizzare la mortalità "infantile" e quella per vecchiaia utilizzando un parametro beta (shape parameter) che permette il

posizionamento in uno dei punti della bathtube curve. Ad esempio un valore β < 1 (0.2-0.6 nel caso di microchip) rappresenta un tasso di mortalità infantile.

Un valore di β=1 indica il periodo di vita normale e quindi quando i valori della distribuzione esponenziale sono piú attendibili. Un valore β>1 modella il periodo oltre il lifetime. Un secondo parametro α(shape) indica quando una certa percentuale della popolazione fallirà, insomma un fattore di scala per la curva (per 3.5 Weibull e' uguale alla distrubuzione gaussiana).

$$f(t) = \frac{\beta}{\alpha}\left(\frac{t}{\alpha}\right)^{\beta-1} e^{-(\frac{t}{\alpha})^{\beta}}$$

Dove t - time-to-failure, ovvero l'intervallo di tempo per cui vale il beta.
Per beta=1 diventa la distribuzione esponenziale:

$$f(t) = \frac{\beta}{\alpha} e^{-(\frac{t}{\alpha})}$$

Non approfondiamo ulteriormente. Abbiamo materiale sufficiente per le maggior parte dei casi. Di fatto dal punto di vista pratico la bathtube curve e quindi la distribuzione di Weibull è un modello che puo' essere utile per pianificare la frequenza iniziale degli interventi di manutenzione e quella successiva ad una certa data.

Failure-rate

Il **failure rate lambda** rappresenta il numero medio di fallimenti per unità di tempo. Durante il periodo di vita utile di un elemento possiamo utilizzare la formula:

$$\lambda = \frac{1}{MTBF}$$

E' un numero tra 0 e 1 quindi possiamo leggerlo come una probabilità. Utilizziamo allora le leggi della probabilità per calcolare il failure-rate di sistemi complessi consistenti di più parti.

La probabilità che due eventi indipendenti si possano verificare in sequenza è:

$$\lambda_{serial} = \lambda_1 + \lambda_2$$

La probabilità che due eventi si possano verificare contemporaneamente è pari al prodotto delle probabilità dei singoli, e questa è la probabilità che entrambi si guastino. Quindi per due dispositivi in parallelo si ha:

$$\lambda_{parallel} = \lambda_1 * \lambda_2$$

Il calcolo di MTBF totale sarà:

$$MTBF(a,b) = \frac{1}{\lambda_{parallel}} = \frac{1}{\lambda_1 * \lambda_2}$$

Nel caso si abbia la MTBF per due dispositivi in serie la formula è:

$$MTBF(a,b) = \frac{1}{\lambda_1 + \lambda_2} = \frac{1}{\frac{1}{mtbf(a)} + \frac{1}{mtbf(b)}}$$

Aumentare l'availability con la ridondanza

Consideriamo una rete di cui sia richiesto il meglio possibile in quanto dev'essere utilizzata 24hx7g. Servizi tipici sono quelli Internet che sono in funzione con continuità. E supponiamo quindi che il nostro servizio internet è importante, potrebbe essere il sito WEB di una banca o di una istituzione o comunque di una grande azienda privata che saprebbe di finire sul giornale anche nel caso di un disservizio di 20 o 30 minuti quali Facebook, Google, Amazon, TIM, Agenzia delle entrate, INPS etc. etc.

Quindi siamo in presenza di servizi per i quali è necessario un valore di availability molto alto.

Il valore availability indica tempo di usabilità del servizio in percentuale del tempo totale. Una availability del 98% equivale a 7,3 giorni di downtime per anno. Al 99% siamo a 3,65 giorni. A 99,99 siamo a 52,56 minuti e a 99,999 siamo a 5,2 minuti.

In base al valore percentuale di uptime voluto si deve progettare l'architettura in modo da avere una availability A, calcolabile con la formula dei paragrafi precedenti, in linea col valore richiesto. Abbiamo bisogno di valori di MTBF e MTTR, ricordiamo la formula:

$$A = \frac{MTBF}{MTBF + MTTR}$$

Come possiamo aumentare l'availability?

Molto banalmente dalla formula si evince che possiamo intervenire abbassando i tempi di riparazione e/o aumentando l'MTBF. Il tempo di manutenzione MTTR negli apparati informatici non sempre si può evitare o prevedere, basti pensare ai bug di sistema. Qui l'unica soluzione è ovviamente quella di ridondare gli apparati in modo di minimizzare il valore di MTTR e alzare il valore di MTBF totale del sistema.

Per i nostri clienti non solo dobbiamo scegliere prodotti con un'alto valore di MTBF ma ci rendiamo conto che l'unica soluzione per incrementarlo consiste nel **ridondare gli apparati**.

Questo è un concetto chiave. Per quanto affidabile e di buona qualità, un singolo dispositivo non può superare una certa soglia di availability. Avrà un guasto, avrà necessità di manutenzione, avrà un problema legato all'ambiente in cui opera.

Abbiamo visto nei paragrafi precendenti che anche un prodotto come uno switch Nexus della Cisco, uno dei migliori sul mercato in termini di affidabilità e qualità, avendo un MTBF di 390000 ore ovvero 44 anni ha una probabilità teorica di guastarsi entro 5 anni dell'11%.

Riprendiamo la formula relativa a due sistemi in parallelo:

$$MTBF(a,b) = \frac{1}{\lambda_{parallel}} = \frac{1}{\lambda_1 * \lambda_2}$$

Da qui traspare che la disponibilità del sistema in parallelo è sempre superiore a quella del singolo componente e si possono ottenere valori molto alti di affidabilità e questa è l'unica strada percorribile in reti che ne richiedono un'altissimo grado.

E' per questa ragione che i più importanti produttori di apparati di networking sono in grado di fornire delle soluzioni ridondate ovvero che consentono di duplicare gli apparati di rete per farli funzionare in parallelo. Le tecnologie VSS e vPC sono ad esempio in uso da Cisco sugli switch di fascia alta, mentre tecnologie come HSRP, VRRP o GLBP si utilizzano normalmente in caso di router. Ovviamente anche altri produttori hanno soluzioni in proposito come Dell, Juniper o altri. Ultimamente ho installato due Cisco Nexus 9500 con doppia scheda supervisor e in cluster tra loro tramite VPC. Quindi due sistemi con 4 schede madri e tre alimentatori ciascuno.

Per aumentare ulteriormente la availability si può andare ancora oltre duplicando geograficamente due datacenter. Due datacenter geograficamente distanti ma ridondati consentono gradi di servizio e affidabilità pari a quelli richiesti dalle più grandi aziende mondiali.

Appendice 1: Esempio di calcolo di MTBF

Qualche considerazione sull'attendibilità dei valori di MTBF forniti dai produttori.

Come calcola un produttore un valore di MTBF? Ci sono degli standard che possono essere seguiti tra cui MIL HDBK-217, Telcordia SR-332 (usato anche da Cisco) o altri.

In ogni caso non è obiettivo di questo documento andare nel dettaglio. Facciamo degli esempi per capirne i principi.

Utilizzare un lab con piú sistemi in parallelo e attendere anni è una opzione non facilmente realizzabile. Calcolare invece un valore numerico, partendo da valori reali dei produttori delle singole parti del sistema è prassi più comune. Il test "sul campo" è verifica di quanto previsto.

Facciamo un esempio.

Un produttore vende 500000 unità di un prodotto in un anno. Immaginiamo un componente con un MTTR pari quasi a zero, come un transceiver di uno switch o un alimentatore. Insomma parti che vanno sostituite e che non sono considerate riparabili. Per MTTF (Medium Time To Failure) si intende il tempo medio tra i guasti. Possiamo considerare:

MTBF = MTTF

in quanto:

$$MTBF = MTTF + MTTR$$

Si possono stimare il numero di ore di utilizzo presso i clienti finali considerando lineare la vendita durante l'anno. Il numero di ore di utilizzo quindi cresce linearmente durante l'anno e solo a fine anno tutte le unità lavoreranno per 24h distribuite nelle location dei clienti che le hanno acquistate.

E' possibile stimare il numero di ore complessivo di utilizzo di tutte le unità vendute partendo dal grafico delle vendite che nel caso piu' semplice e' una retta che unisce i punti (0,0) e (365,500000). Il numero di ore complessivo di utilizzo delle unità sarà l'area al di sotto del triangolo definito da questo segmento. Utilizzando l'equazione della retta che passa per questi punti e integrando si ottiene il dato richiesto.

Da un calcolo ne consegue che il numero totale di ore di lavoro di queste unità in un anno e' la metà del numero di ore disponibili in quell'anno. Intuitivamente c'e' il fatto che a metà anno il 50% sono vendute e lavorano

per 24h. Prima e dopo questa data in modo simmetrico si compensano a vicenda.

Il numero totale di ore è:

$$\frac{500000 * (24h * 365gg)}{2} = (2{,}19 * 10^9)h$$

In questo periodo supponiamo 900 unità vengano restituite perche' guaste. Quindi possiamo dedurre:

$$MTBF = \frac{T}{F} = \frac{2{,}19 * 10^9}{900} = 243 * 10^4 = 277anni$$

Cioè se hai 277 apparati attivi nel corso di un anno in media uno di questi si guasterà durante l'anno. Ricordiamo che è un valore medio tanto più attendibile quanto è maggiore il numero di unità.

Questo metodo del calcolo del MTBF è utilizzato in alcuni casi dai produttori per verificare dati teorici.

Il valore di MTBF è molto più lungo del lifetime, in genere di 8-10 volte per i prodotti IT quali router o switch. E' chiaro che questi valori sono calcolati considerando i prodotti operare in condizioni ideali.

Considerate il fatto che un componente elettronico un media può avere un lifetime di 10 anni. Andando a ritroso si può comprendere perchè nel mondo reale un produttore di router/switch ti consiglia di sostituire i prodotti ogni 3/5 anni in quanto ti deve garantire un periodo di tempo in cui la probabilità di guasto sia sufficientemente bassa.

Qualcuno potrebbe pensare che i produttori utilizzano i clienti quale piattaforma di test per i nuovi prodotti. Ma questa è la ragione per cui esiste una garanzia per ogni prodotto da parte di un produttore e il motivo per cui esistono i "richiami" gratuiti dei prodotti per la sostituzione di parti con una percentuale di guasti superiore a quanto previsto.

Appendice 2: Esempio di calcolo di availability

Consideriamo un sistema ridondato e quindi progettato per avere un buon valore di availability. In tal caso si installa sempre un sistema di router/switch ridondati. Consideriamo due switch L3 in parallelo tramite una tecnologia quale lo stack oppure il Cisco VPC.

Possiamo porre il valore di MTTR pari a zero in quanto stiamo progettando un sistema ridondato che permette una manutenzione senza creare disservizio. In un sistema sistemi ridondato c'e' una sorta di riparazione automatica in cui si passa subito dal sistema guasto a quello effettivo (schede ridondate).

I dispositivi ridondati sono identici e quindi con lo stesso valore di MTBF e questo ci consente di usare le formule presentate.

Ecco la dotazione hardware:

- Cisco chassis Nexus 9504 con un MTBF di 1038080 ore (118anni).
- La supervisor N9K-SUP-A con un MTBF di 312000 ore (35anni).
- La scheda controller N9K-SC-A ha un MTBF di 1380210 ore (157 anni)
- L'alimentatore AC ha un MTBF di 868870 ore (99 anni)

Nel caso di un sistema modulare possiamo immaginare gli elementi come posti in serie nel momento in cui il guasto di uno di essi blocca l'intero sistema quindi consideriamo il caso di moduli non ridondati.

Nel caso di un Cisco chassis 9504 con un alimentatore, una supervisor e un controller non ridondati che consideriamo in serie tra loro:

$$MTBF = \frac{1}{\lambda 1 + \lambda 2 + \lambda 3 + \lambda 4} = \frac{1}{\frac{1}{118} + \frac{1}{35} + \frac{1}{157} + \frac{1}{99}} \approx 18{,}9y$$

Il risultato sorprendente è dovuto al fatto che qui la catena sarà più debole del suo anello più fragile e il valore 312000 della supervisor ne è una indicazione. Questo valore più basso probabilmente è dovuto alla complessità dei componenti presenti essendo assimilabile ad una server motherboard. Quindi è il primo modulo da ridondare (interessante notare un MTBF inferiore all'alimentatore).

Quindi è importante ridondare la supervisor N9K-SUP-A, anche perchè si tratta di un modulo soggetto a frequenti manutenzioni, basti pensare alle patch e agli aggiornamenti di software.

Due supervisor sono due moduli in parallelo identici. Cerchiamo di calcolarne il valore MTFB. La probabilità che due eventi indipendenti si possano verificare contemporaneamente è pari al prodotto delle probabilità dei singoli, e questa è la probabilità che entrambi si guastino. Se la probabilità che uno si guasta è lambda, quella che si guastino entrambi è lambda^2 quindi 0,0285^2=0,000812 che sostituto nella formula di sopra da un MTBF=39,08y ovvero di molto superiore. Quindi stiamo calcolando la probabilità che si guastano entrambe, patendo dal presupposto che il guasto del singolo modulo non crei problemi al sistema.

Ridondando gli altri elementi dello chassis e se necessario raddoppiando gli chassis si possono ottenere dei valori di affidabilità decisamente elevati.

Per un cliente particolare ho installato due Cisco 9500 con triplo alimentatore, doppia supervisor e doppia scheda controller. Riutilizzando la formula di cui sopra, con le dovute approssimazioni ottengo nel caso di singolo dispositivo con triplo alimentatore e doppie schede:

$$MTBF = \frac{1}{\lambda 1 + \lambda 2 + \lambda 3 + \lambda 4} = \frac{1}{\frac{1}{118} + \left(\frac{1}{35}\right)^2 + \left(\frac{1}{157}\right)^2 + \left(\frac{1}{99}\right)^3} \approx 107y$$

Nel caso di due Nexus in parallelo avremo:

$$MTBF(sup1, sup2) = \frac{1}{\lambda_1 * \lambda_2} = \frac{1}{\frac{1}{107} * \frac{1}{107}} = 11449\text{y}$$

ecco cosa possiamo aspettarci dopo 11anni che la macchina è operativa ovvero a 1/1000 di MTBF:

$$R(t) = e^{-t/MTBF} = e^{-11/11449} \approx 0{,}999$$

Quindi c'e' il 99,9% di probabilità che al tempo T=11y il sistema funzioni.

Stiamo considerando un sistema con un tempo di riparazione pari a zero, questa è una semplificazione eccessiva nel caso di sistemi singoli ma accettabilissima in caso di sistemi con ridondanze come quello in questo esempio.

Il cliente ovviamente deve sapere che i nostri calcoli non comprendono disservizi dovuti a errori umani nella configurazione degli apparati, gravi bug di sistema, problemi di alimentazione o di condizionamento, o tempi di

riparazione talmente lunghi da aumentare le probabilità di più guasti contemporanei.

Il modello supervisor N9K-SUP-A+ ha un MTBF di 414240 ore (47y). In questo caso due moduli in parallelo ci darebbero un valore:

$$MTBF(sup1, sup2) = \frac{1}{\lambda_1 * \lambda_2} = \frac{1}{\frac{1}{47} * \frac{1}{47}} = 2209\text{y}$$

Nel nostro sistema dovremmo anche aggiungere un modulo ethernet come minimo tipo N9K-X97160YC-EX con 440000 di MTBF, non ridondato perche' uno per ogni chassis con ridondanza delegata ai server collegati. Tuttavia se ne consideriamo due per chassis per allinearci ai calcoli fatti sino ad ora avremmo invece di un 107y un valore di circa 102y.

Fine documento